



ÉVALUEZ PRÉCISEMENT VOTRE RISQUE AVANT QU'IL NE DEVIENNE RÉALITÉ

SERVICES PROFESSIONNELS DE CYBERSÉCURITÉ

UNE APPROCHE GLOBALE ET SYSTÉMATIQUE DE LA GESTION DU RISQUE ET DE LA PROTECTION DES INFRASTRUCTURES STRATÉGIQUES

BÂTIR DES RÉSEAUX PLUS RÉILIENTS À L'ÈRE DE L'AUGMENTATION DES CYBER-ATTAQUES

Le monde numérique a donné naissance à de nouvelles manières d'accroître la productivité, de maximiser la valeur et, au final, d'améliorer la vie de milliards de personnes. Parallèlement à cela, l'explosion du nombre d'incidents de cyber-sécurité confronte les entreprises et les organismes gouvernementaux à des défis uniques. Aujourd'hui, les attaques polymorphes, capables de se modifier elles-mêmes à chaque exécution, sont devenues monnaie courante. Bien que de nombreuses organisations se persuadent que leurs informations stratégiques confidentielles sont inoculées, il devient chaque jour plus manifeste que personne n'est immunisé. La notion de cyber-sécurité s'étend bien au-delà des attaques de pirates informatiques et des contrôles techniques.

En outre, l'environnement réglementaire et applicatif de la cyber-sécurité est dynamique ; son évolution rapide engendre de nouveaux défis en contraignant les entreprises à se conformer à une multitude de normes industrielles, tout en appliquant des contrôles de sécurité appropriés. À mesure que les réseaux stratégiques se transforment en systèmes dynamiques, constitués de réseaux interconnectés reposant sur des plates-formes ouvertes et des solutions dans le Cloud, une gouvernance et une supervision deviennent indispensables tout au long du cycle de vie opérationnel du système. Cela inclut une réévaluation coordonnée et régulière des personnes, des processus et des technologies, afin de garantir que le niveau de préparation de l'organisation lui permet de se protéger, mais également de détecter et réagir à des menaces changeantes.





COMPRENDRE VOTRE PROFIL DE RISQUE DE CYBERSÉCURITÉ

Les services de cyber-sécurité professionnels de Motorola fournissent un processus complet et systématique dédié à l'identification, l'évaluation et la gestion du risque de cyber-sécurité dans tous les systèmes d'entreprise. Avec les services de cyber-sécurité professionnels, vous serez en mesure de pleinement comprendre votre profil de risque de cyber-sécurité en fonction de l'environnement opérationnel de votre organisation. Motorola fournit une évaluation exhaustive de votre surface d'attaque, ainsi qu'une évaluation des coûts/avantages et des préconisations correctives détaillées. Face à des technologies et des processus métier toujours changeants, les menaces de sécurité évoluent constamment, et la posture de sécurité de votre organisation n'est jamais statique. L'évaluation périodique de la posture de sécurité permet de disposer d'un inventaire actuel des vulnérabilités et de hiérarchiser les mesures correctives requises en fonction du risque global pour votre activité.

En 2014, le National Institute of Standards and Technology (NIST) a publié le document « Framework for Improving Critical Infrastructure Cybersecurity », un cadre de référence destiné à aider les organisations à atteindre leurs objectifs en matière de cyber-sécurité. Ce cadre de référence comprend des pratiques préconisées par différents organismes de normalisation, dont la mise en œuvre a été couronnée de succès. Motorola Solutions a contribué, aux côtés de partenaires gouvernementaux et industriels, à l'élaboration de ce cadre de référence. L'évaluation de Motorola repose donc sur les préconisations du NIST, en recoupant le cadre de référence en matière de cyber-sécurité du NIST avec les procédés et procédures actuels de gestion du risque de votre organisation, pour déterminer le niveau de risque de votre profil de cyber-sécurité et formuler des préconisations.

CADRE DE RÉFÉRENCE DE CYBERSÉCURITÉ DU NIST

 IDENTIFIER	 PROTÉGER	 DÉTECTER	 RÉAGIR	 RÉCUPÉRER
Environnement métier Gouvernance du risque Gestion des ressources Évaluation du risque Gestion du risque	Stratégies Procédés Sécurité des données Contrôle d'accès Technologie de protection Sensibilisation et formation	Anomalies et événements Procédés de détection Surveillance continue	Planification de la réponse Communications Analyse Atténuation Améliorations	Planification de la reprise Améliorations Communications

Les infrastructures stratégiques sont variées et complexes. Ces systèmes doivent être sécurisés et doivent pouvoir être rétablis rapidement après tout incident, notamment après un incident physique ou de sécurité. Nos initiatives de réduction des risques et nos activités de gestion reposent sur l'identification des ressources ; l'évaluation du risque en fonction des conséquences, des vulnérabilités et des menaces ; l'établissement de priorités pour atténuer les risques ; la mise en œuvre de programmes de protection et la mesure de l'efficacité.

AMÉLIORER LA GESTION DU RISQUE EN IDENTIFIANT ET EN RÉDUISANT LES MENACES

Au terme de plusieurs années de coopération avec des clients issus des secteurs de la sûreté publique, du gouvernement et de l'entreprise, l'équipe des services de cyber-sécurité professionnels de Motorola a développé une approche globale et méthodique de la gestion du risque pour offrir des résultats exhaustifs, informatifs et hiérarchisés en fonction du risque. Les propriétaires de risque et les décideurs reçoivent une évaluation factuelle, calculée avec soin, des facteurs de risque applicables.

PORTÉE	Seuls les contrôles pertinents, couvrant aussi bien la technique que la gestion et l'exploitation, sont sélectionnés pour réaliser une analyse personnalisée du risque. Des mesures d'atténuation telles que la modification de l'architecture, l'intégration de produits spécifiques ou la mise en œuvre de contrôles procéduraux sont préconisées et évaluées avec les différents intervenants, uniquement après l'évaluation méthodique de l'environnement, l'identification, l'analyse et la compréhension des risques et la hiérarchisation des risques.
APPROCHE	Motorola recourt à l'observation physique, aux entretiens en personne ainsi qu'à des outils manuels, informatisés, disponibles dans le commerce et conçus sur mesure pour évaluer les scénarios de menace et étudier les risques potentiels en termes de confidentialité, d'intégrité et de disponibilité de la mission de l'organisation.
MÉTHODOLOGIE	Tous les facteurs de risque pertinents sont examinés et pris en compte avant et pendant l'évaluation. Après la capture de toutes les données nécessaires dans le cadre de l'évaluation, un profil de menace est établi et préparé sous la forme d'un rapport de notation du risque, comportant une valeur faible, modérée, élevée ou critique pour chaque diagnostic ou problème identifié. Une préconisation corrective ou une recommandation d'acceptation du risque est formulée pour chaque diagnostic ou problème.

DISCIPLINES DES SERVICES PROFESSIONNELS DE CYBERSÉCURITÉ

GESTION

- Analyse des répercussions sur l'activité
- Identification et classification des ressources
- Évaluation de la préparation, conformément au cadre de référence du NIST
- Structure et institutionnalisation de la gouvernance, conformément au cadre de référence
- Fiche de notation des risques de cyber-sécurité et indicateurs de performances-clés (KPI) de l'organisation
- Élaboration d'une stratégie et de normes à l'échelle de l'organisation
- Efficacité des processus opérationnels
- Modélisation et connaissance des menaces
- Évaluation du risque pour la propriété intellectuelle
- Évaluation du risque pour la production et le développement de logiciels décentralisés
- Cycle de vie de développement sécurisé
- Analyse/recherche de menaces
- Évaluation des répercussions sur la conformité réglementaire
- Procédé et stratégie de gestion de fournisseurs tiers
- Formation et sensibilisation

OPERATIONAL

- Demandes de renseignements de clients ad hoc
- Assistance à la sécurité opérationnelle
- Assistance à la réponse en cas d'incident
- Enquête et investigation numérique
- Surveillance sur mesure de la sécurité
- Surveillance sur mesure de la détection d'anomalies
- Tests d'ingénierie sociale

CRITÈRES TECHNIQUES

- Évaluations des risques techniques pour la cyber-sécurité
 - Analyses des vulnérabilités
 - Sécurité des applications Web
 - Tests de pénétration des réseaux locaux et sans fil
 - Tests de pénétration physique
 - Évaluation du déploiement dans le Cloud
- Évaluation de la conformité
- Examen de l'architecture du réseau
- Solutions de gestion des identités et des accès
- Évaluation de la connectivité de tiers
- Évaluation du risque des environnements SCADA
- Découverte du réseau/inventaire des ressources
- Vérification des applications/examen du code
- Architecture de référence de sécurité
- Sécurité de l'architecture d'entreprise
- Services de cryptographie
- Adoption de technologies mobiles sécurisées
- Déploiement et surveillance d'appâts
- Conformité des licences en open source

OPTIONS DE FOURNITURE DE SERVICES PROFESSIONNELS DE CYBERSÉCURITÉ

Les services de cyber-sécurité professionnels de Motorola sont fournis par une équipe de professionnels certifiés de la sécurité, formés et activement informés sur l'évolution rapide de l'environnement des menaces de sécurité et des technologies de conformité. Nous collaborerons avec vous afin d'établir la meilleure méthodologie d'évaluation pour atteindre vos objectifs opérationnels souhaités. Les options disponibles incluent :

EXÉCUTION PAR MOTOROLA SOLUTIONS

L'équipe des services de cyber-sécurité professionnels de Motorola procède à une évaluation complète et fournit des recommandations hiérarchisées selon le risque.

ENGAGEMENT COMMUN

Motorola supervise l'engagement en travaillant avec votre personnel informatique pour garantir la viabilité du programme, le partage d'informations et la collaboration des experts.

COORDINATION DE TIERCES PARTIES INDÉPENDANTES

Une tierce partie réputée, désignée pour réaliser une évaluation impartiale avec la supervision de MSI, pour garantir l'exécution et la fourniture et répondre à vos objectifs.

Notre évaluation des risques cyber-sécurité est incluse dans les services fournis aux clients de nos services Premier, et peut être réalisée à la demande pour d'autres clients.

COMPTEZ SUR MOTOROLA SOLUTIONS POUR VOS SERVICES DE GESTION PROACTIVE DU RISQUE DE CYBERSÉCURITÉ

En tant que leader mondial et fournisseur de technologies sécurisées à des activités stratégiques dans plus de 100 pays, nous comprenons parfaitement l'importance de la conception, du développement et du déploiement des technologies innovantes les plus efficaces et sécurisées.

Les clients ont des attentes grandissantes et exigent une approche plus globale de la cybersécurité tout au long des cycles de développement, de mise en œuvre et d'exploitation d'une solution. Les progrès technologiques dans le domaine des communications stratégiques génèrent une surface d'attaque plus importante, qui peut vous rendre vulnérable aux incidents de sécurité.

Vos systèmes stratégiques sont considérés comme des cibles à forte valeur par les cybercriminels, dont la connaissance de la technologie progresse continuellement. Ces tendances cumulées engendrent des risques accrus en termes de disponibilité, de confidentialité et d'intégrité de vos communications voix et données stratégiques. Adopter une approche globale de la sécurité des systèmes, reposant sur la détection proactive des menaces, une capacité de réaction en temps réel et des mesures correctives, vous offre la sérénité de savoir que votre système est à la fois sécurisé et résilient.

Pour plus d'informations sur nos services de cyber-sécurité professionnels, contactez votre représentant Motorola ou consultez le site Web motorolasolutions.com/cybersecurity

Motorola Solutions France SAS Parc Les Algorithmes Saint Aubin 91193 Gif-sur-Yvette, France motorolasolutions.fr

MOTOROLA, MOTO, MOTOROLA SOLUTIONS et le logo M stylisé sont des appellations commerciales ou des marques déposées de Motorola Trademark Holdings, LLC et sont utilisées sous licence. Les autres marques sont la propriété de leurs détenteurs respectifs. © 2017 Motorola, Inc. Tous droits réservés. 1217